REMARKS

Claims 1-20 are pending. Claims 1, 10, and 20 have been amended. Claims 3 and 12 have been canceled. Claims 1, 2, 4-11, and 13-20 remain in this application.

Pursuant to 37 C.F.R. 1.116(b), Claims 1, 10, and 20 have been amended to present the claims in better form for consideration on appeal. Specifically, these claims have been amended to incorporate the limitations in now-canceled Claims 3 and 12. In addition, support for the amendments can be found in the specification on page 10, lines 3-13 and 18-23. No new matter has been introduced. Entry of the claim amendments is requested.

Claims 1-20 again stand rejected under 35 U.S.C. §103(a) as being obvious over U.S. Patent No. 6,357,008, issued to Nachenberg ("Nachenberg"), and further in view of U.S. Patent No. 6,314,425, issued to Serbinis et al. ("Serbinis"). Applicant traverses the rejection.

To establish a *prima facie* case of obviousness: (1) there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or combine the reference teachings; (2) there must be a reasonable expectation of success; and (3) the combined references must teach or suggest all the claim limitations. MPEP § 2143. A *prima facie* case of obviousness has not been shown with respect to Claims 1, 10, and 20.

As previously argued, the Nachenberg patent discloses a method for detecting computer viruses through decryption, exploration and evaluation using emulation and artificial intelligence (Abstract; Col. 1, lines 16-20). During decryption, a sufficient number of instructions are emulated to allow an encrypted virus to decrypt the viral body of the encrypted virus (Col. 7, lines 3-5). During exploration, all sections of code within a region likely to contain any virus are emulated (Col. 7, lines 9-11). During evaluation, any suspicious operations observed during the decryption and exploration phases are analyzed to determine whether the target program appears to be infected by a computer virus (Col. 7, lines 17-20). Nachenberg also discloses static heuristic virus detection that

involves searching the instructions of a target program of instruction sequences that perform operations typically used by computer viruses (Col. 2, lines 39-45). By way of background, the Nachenberg patent distinguishes over signature scanning antivirus programs that can identify particular virus strains for removal and which may have a low "false-positive" rate (Col. 1, lines 39-42). Only viruses whose signatures have already been determined and stored in a signature database may be detected using signature scanning (Col. 1, lines 42-46).

In contrast, the Serbinis reference discloses an apparatus and method for use of access tokens in an Internet document management system over open networks programmed to generate the access tokens and to provide a plurality of document management services (Abstract; Col. 1, lines 11-14; Col. 5, lines 2-6). The document management services include document storage and retrieval, collaborative file sharing, workflow services for electronic documents, an electronic document delivery service, and a document distribution service (Col. 5, lines 4-8). The Serbinis reference includes a relational database (Col. 6, lines 37-52), which utilizes a hierarchical storage schema (Col. 8, lines 12-24). Access to the system and services are controlled through the use of access tokens (Abstract). Each access token is a security code comprised of a signed string unique to a transaction and generated from one or more random numbers independent of any user information, resource information, or other identifiable information (Col. 5, lines 9-14).

The required burden to prove a *prima facie* case of obviousness has not been shown. First, Nachenberg fails to provide a suggestion or motivation to combine with the reference teachings of Serbinis. In general, Nachenberg teaches a method for detecting computer viruses using a dynamic heuristic approach to detecting viruses. Nachenberg also distinguishes over signature scanning anti-virus programs, but such reference fails to provide a suggestion or motivation to combine with Serbinis. While Nachenberg recognizes that virus signatures have already been determined are stored in a signature database, Serbinis teaches storing documents without teaching that such documents themselves concern virus data. Obviousness may not be established by picking and choosing from an

art reference only so much of the reference as will support a given position, to the exclusion of other parts necessary to the full appreciation of what such reference fairly suggests to one of ordinary skill in the art. *Bausch & Lomb, Inc. v. Barnes-Hind, Inc.*, 796 F.2d 443, 230 USPQ 416 (Fed. Cir. 1986). Documents that might contain viruses are not the same as documents containing information about viruses, the latter of which is neither taught nor suggested by Serbinis. Thus, Serbinis' reference to scanning documents for viruses does not teach that storing documents is a necessary or desirable part of detecting viruses. Nor does Serbinis teach or suggest the storing of virus signatures. As a result, one of ordinary skill in the art would not perceive any reason to combine the Internet-based document management system of Serbinis with the dynamic heuristic virus detection method of Nachenberg.

Second, one of ordinary skill in the art would not have a reasonable expectation of success in combining the teachings of Nachenberg and Serbinis. Nachenberg teaches a dynamic heuristic approach whose chief advantage is detecting new or previously-undiscovered viruses and distinguishes over signature scanning anti-virus programs that work by scanning files for signatures of known viruses. Serbinis, which is concerned with providing access tokens in an Internet-based document management system, discloses no form of virus detection. If Nachenberg were to be combined with Serbinis, the result would be a dynamic heuristic virus detection method, wherein records containing only virus identification information would be available over the Internet to selected users possessing appropriate access tokens. Given that Nachenberg fails to teach or suggest maintaining virus information records, why or how such combination would be desirable or useful is speculative.

Finally, even if combined, the Nachenberg and Serbinis references fail to teach or suggest all claim limitations. Finding similar elements in one or more references does not render an invention automatically unpatentable, and the invention itself may not be used as an instruction book on how to reconstruct the invention from the art references. *See Panduit Corp. v. Dennison, Mfg. Co.*, 810 F.2d 1561, 1 USPQ2d 1593 (Fed. Cir. 1987).

Initially, Nachenberg is primarily concerned with detecting new or previously-undiscovered viruses. Accordingly, Nachenberg fails to teach or suggest such claim elements as a virus removal sentence *comprising object code* providing operations to clean the identified computer virus within a computer system or a virus removal sentence *comprising object code* providing operations to clean the identified computer virus from the computer system, per Claims 1, 10 and 20 (emphasis added). Similarly, Nachenberg fails to teach or suggest binary data encoding instructions to clean the computer virus from the computer system, wherein the instructions *comprise the object code* to clean the identified computer virus, per Claims 1, 10 and 20 (emphasis added). Although Nachenberg indicates that "a signature scanning antivirus program can identify particular virus strains for removal" (Col. 1, lines 39-40), Nachenberg fails to teach or suggest with any degree of specificity how the actual virus removal should be accomplished. Moreover, Nachenberg fails to teach or suggest comparing subsequently modified versions of the structured virus database to form a delta set of virus definition records and storing the delta virus definition records set into the structured virus database. Rather, Nachenberg merely states that when "the antivirus main module 151 is set to scan a target program . . . to determine heuristically whether or not the target program contains virus-like code, the main module 151 begins the decryption phase . . .." (Col. 7, lines 24-27).

Similarly, Serbinis fails to teach or suggest converting virus definition records into a virus data file comprising virus definition sets or binary data encoding instructions to detect the computer virus within a computer system, wherein the instructions *comprise the object code* to detect the identified computer virus, per Claims 1, 10 and 20. Serbinis teaches that, if desired, documents can be scanned for viruses before being stored, but fails to teach or suggest a virus definition set or binary data encoding instructions. Accordingly, all claim limitations are not found in Nachenberg and Serbinis.

In view of the foregoing, no suggestion or motivation exists to combine the teachings of Nachenberg with those of Serbinis, there would be no expectation of success if the teachings were combined, and (3) the combined references fail to

teach or suggest all the claim limitations. Thus, a *prima facie* case of obviousness has not been shown with respect to Claims 1, 10 and 20.

Claims 3 and 12 have been canceled and no longer remain in the applications. Claims 2 and 4-9 are dependent on Claim 1 and are patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. Claims 11 and 13-19 are dependent on Claim 10 and are patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. As a *prima facie* case of obviousness has not been shown, withdrawal of the rejection of Claims 1-20 for obviousness under 35 U.S.C. 103(a) is requested.

The prior art made of record and not relied upon has been reviewed by the applicant and is considered to be no more pertinent than the prior art references already applied.

Claims 1, 2, 4-11, and 13-20 are believed to be in a condition for allowance. Withdrawal of the finality of the Office action and entry of the foregoing amendments is respectfully requested. A Notice of Allowance is earnestly solicited. Please contact the undersigned at (206) 381-3900 regarding any questions or concerns associated with the present matter.

Respectfully submitted,

Dated: June 10, 2005

By: _____
Kevin J. Zilka
Reg. No. 41,429

Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120

Telephone: (408) 971-2573
Facsimile: (408) 971-4660